FIG.1

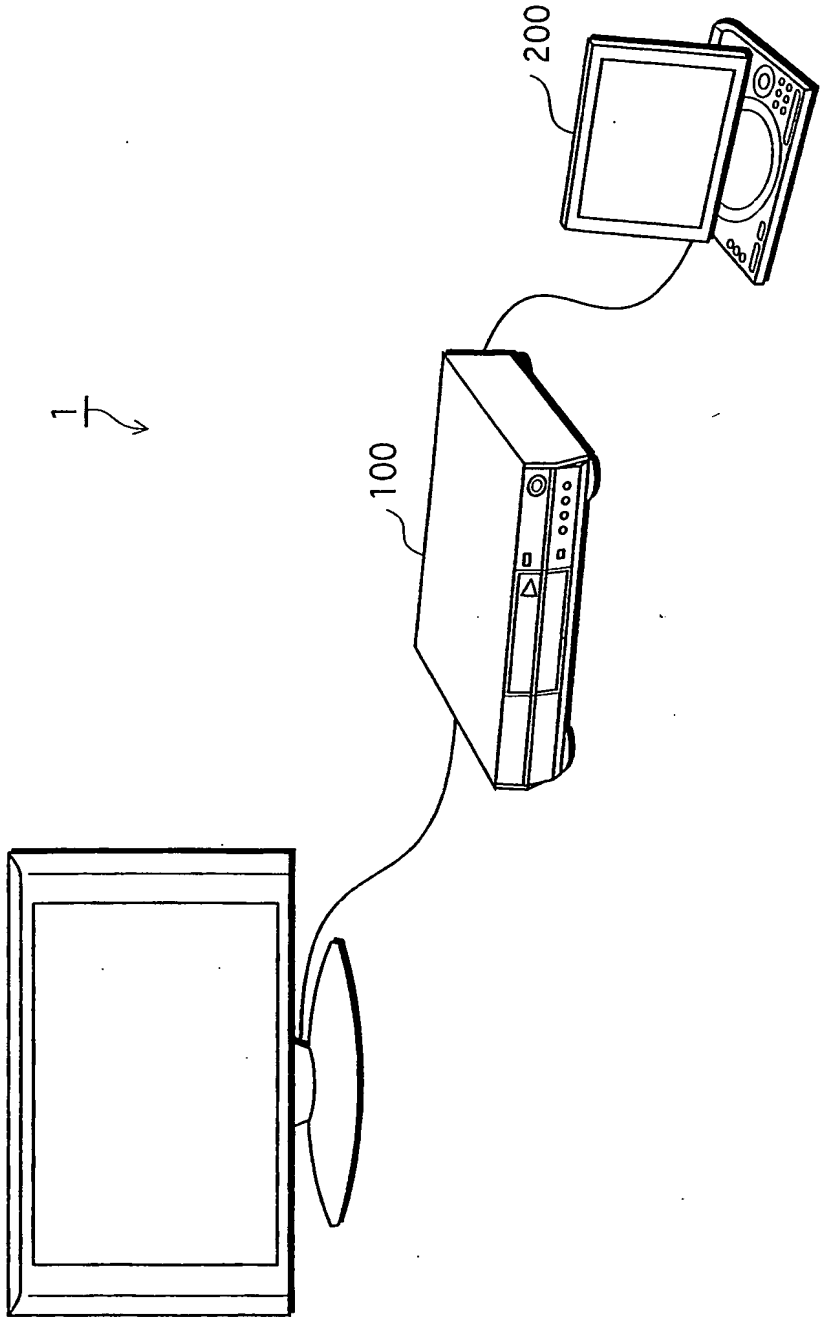


FIG.2

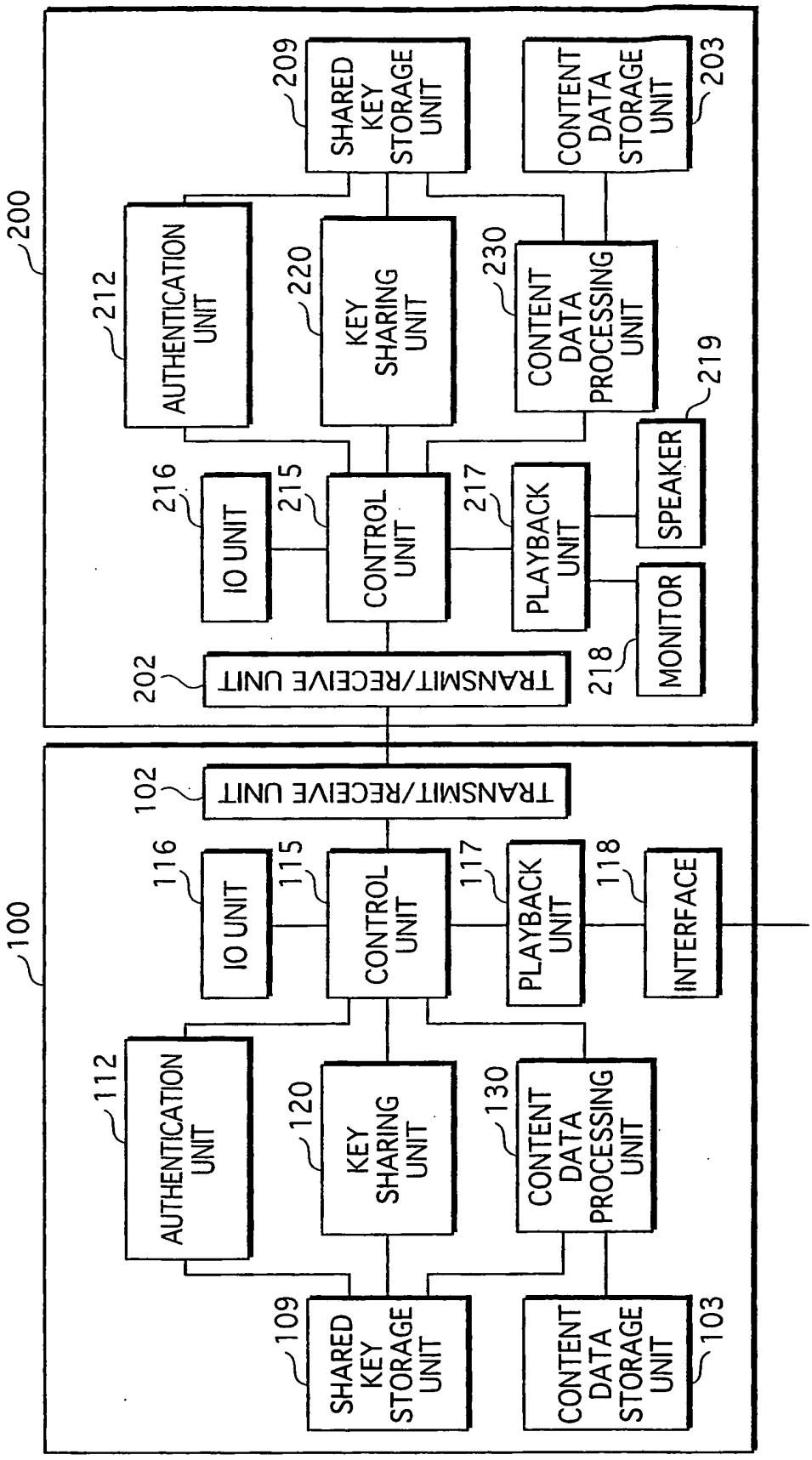

200
209
SHARED KEY STORAGE UNIT
CONTENT DATA STORAGE UNIT
203
212
AUTHENTICATION UNIT
220
KEY SHARING UNIT
230
CONTENT DATA PROCESSING UNIT
219
216
IO UNIT
215
CONTROL UNIT
217
PLAYBACK UNIT
SPEAKER
202
TRANSMIT/RECEIVE UNIT
218
MONITOR
100
102
TRANSMIT/RECEIVE UNIT
116
IO UNIT
115
CONTROL UNIT
117
PLAYBACK UNIT
118
INTERFACE
112
AUTHENTICATION UNIT
120
KEY SHARING UNIT
130
CONTENT DATA PROCESSING UNIT
109
SHARED KEY STORAGE UNIT
CONTENT DATA STORAGE UNIT
103

FIG.3

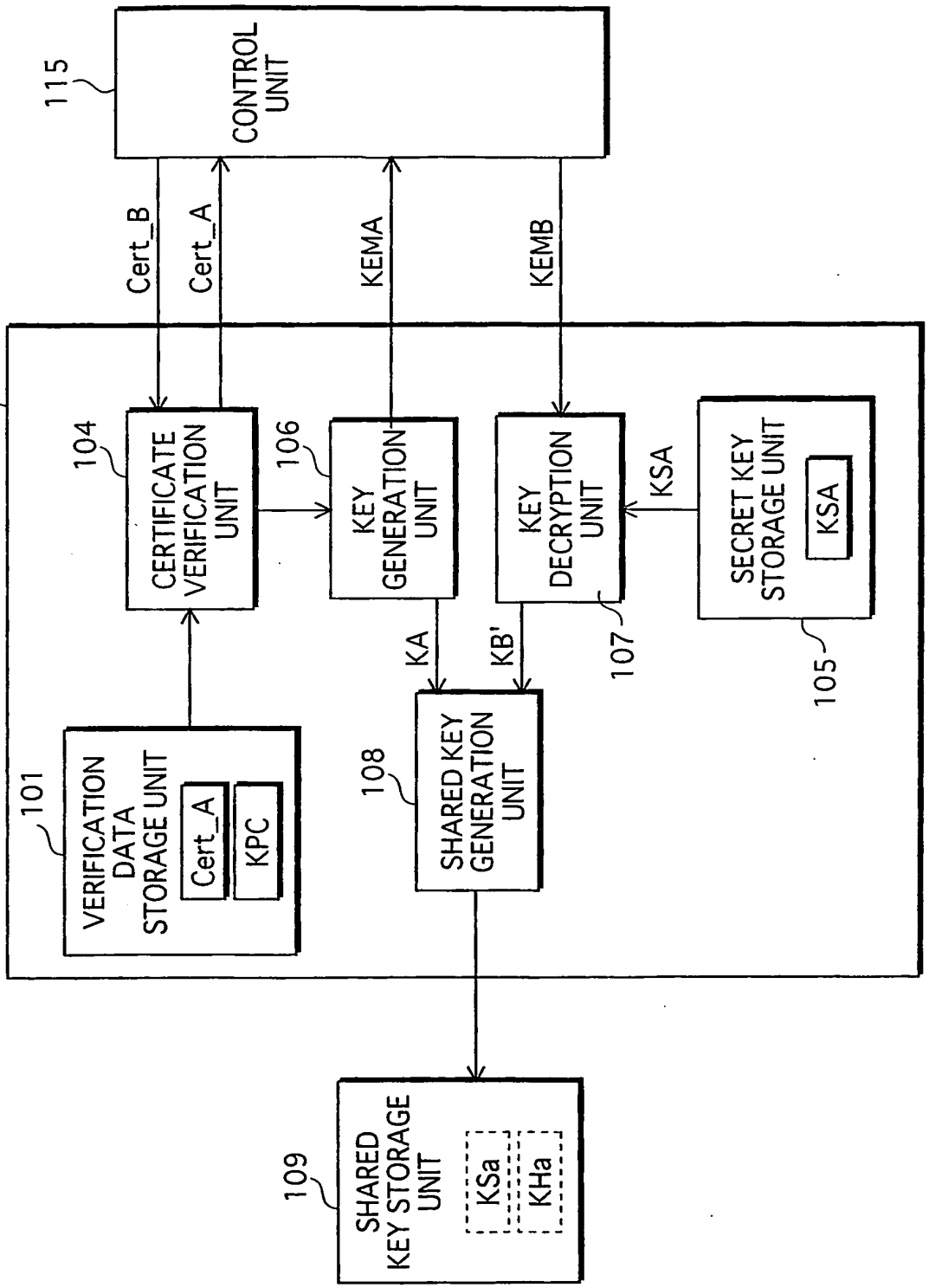

115
CONTROL UNIT
Cert_B
Cert_A
KEMA
KEMB
120
104
CERTIFICATE VERIFICATION UNIT
106
KEY GENERATION UNIT
KEY DECRYPTION UNIT
KSA
SECRET KEY STORAGE UNIT
KSA
105
107
KA
KB'
101
VERIFICATION DATA STORAGE UNIT
Cert_A
KPC
108
SHARED KEY GENERATION UNIT
109
SHARED KEY STORAGE UNIT
KSa
KHa

FIG.4

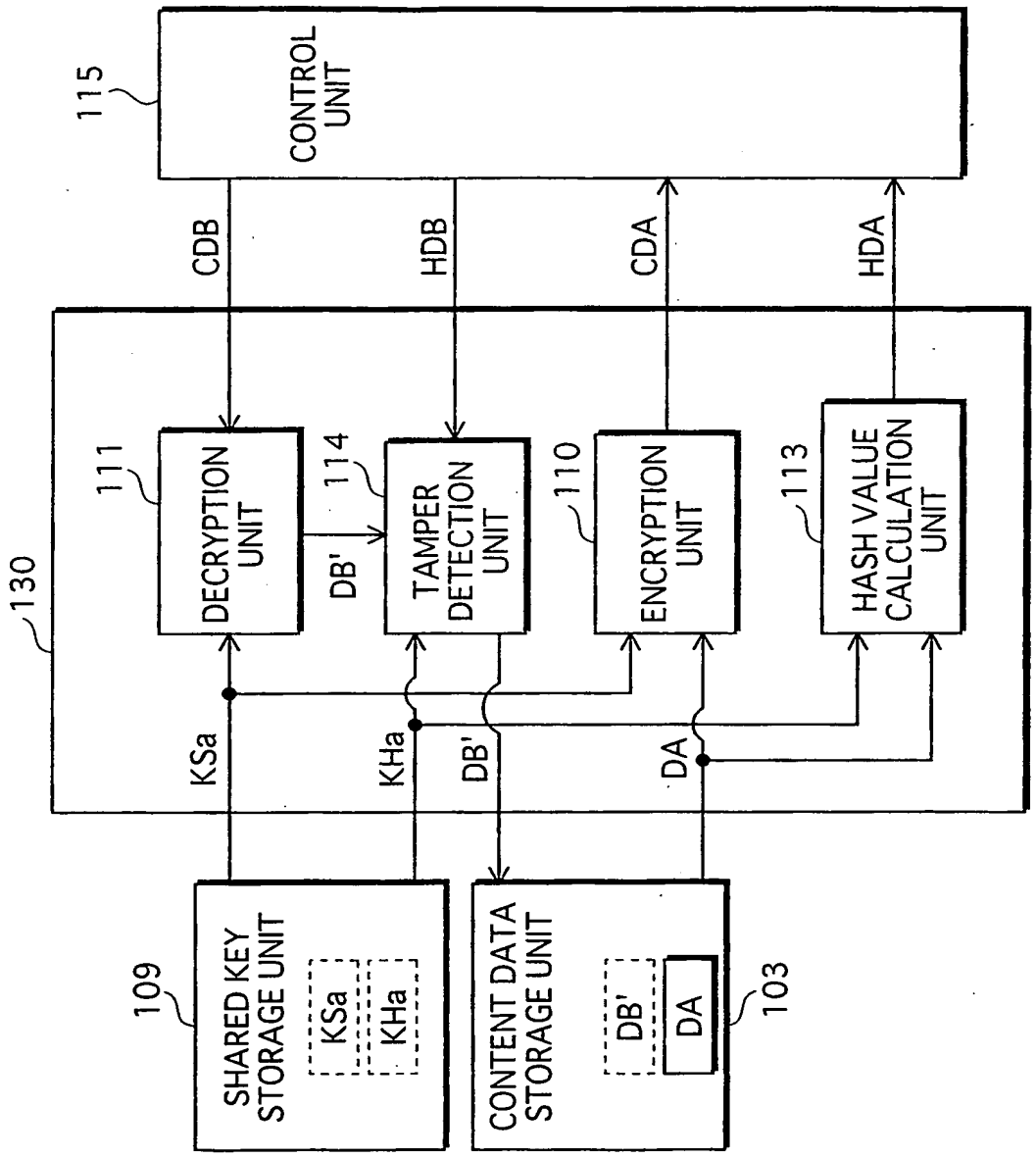

115
CONTROL UNIT
CDB
HDB
CDA
HDA
130
111
DECRYPTION UNIT
DB'
114
TAMPER DETECTION UNIT
110
ENCRYPTION UNIT
113
HASH VALUE CALCULATION UNIT
KSa
KHa
DB'
DA
109
SHARED KEY STORAGE UNIT
KSa
KHa
CONTENT DATA STORAGE UNIT
DB'
DA
103

FIG.5

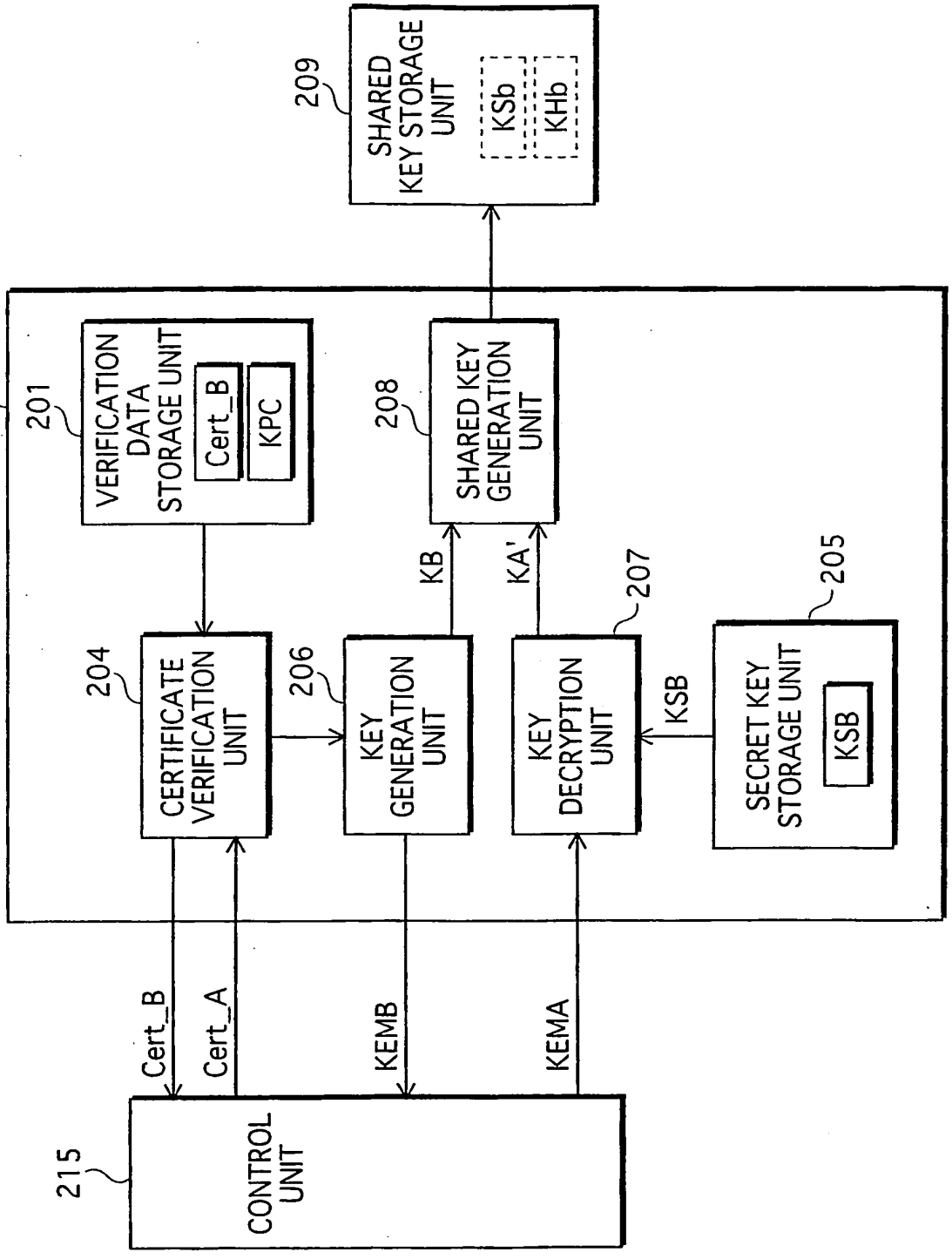

209
SHARED KEY STORAGE UNIT
KSb
KHb
220
201
VERIFICATION DATA STORAGE UNIT
Cert_B
KPC
208
SHARED KEY GENERATION UNIT
KB
KA'
207
205
204
CERTIFICATE VERIFICATION UNIT
206
KEY GENERATION UNIT
KEY DECRYPTION UNIT
KSB
SECRET KEY STORAGE UNIT
KSB
Cert_B
Cert_A
KEMB
KEMA
215
CONTROL UNIT

FIG.6

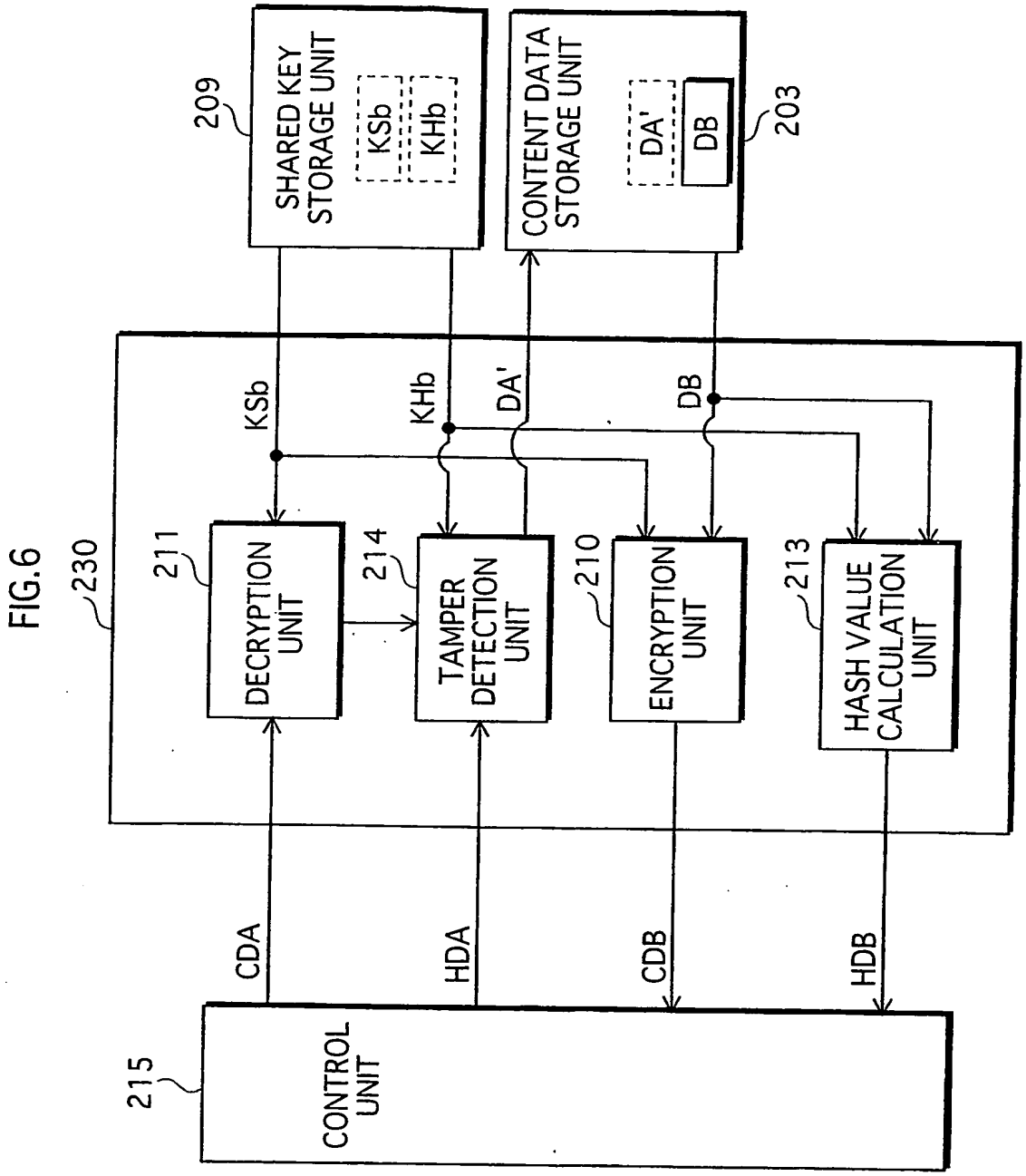

209
SHARED KEY STORAGE UNIT
KSb
KHb
CONTENT DATA STORAGE UNIT
DA'
DB
203
KSb
KHb
DA'
DB
230
211
DECRYPTION UNIT
214
TAMPER DETECTION UNIT
210
ENCRYPTION UNIT
213
HASH VALUE CALCULATION UNIT
CDA
HDA
CDB
HDB
215
CONTROL UNIT

FIG.7

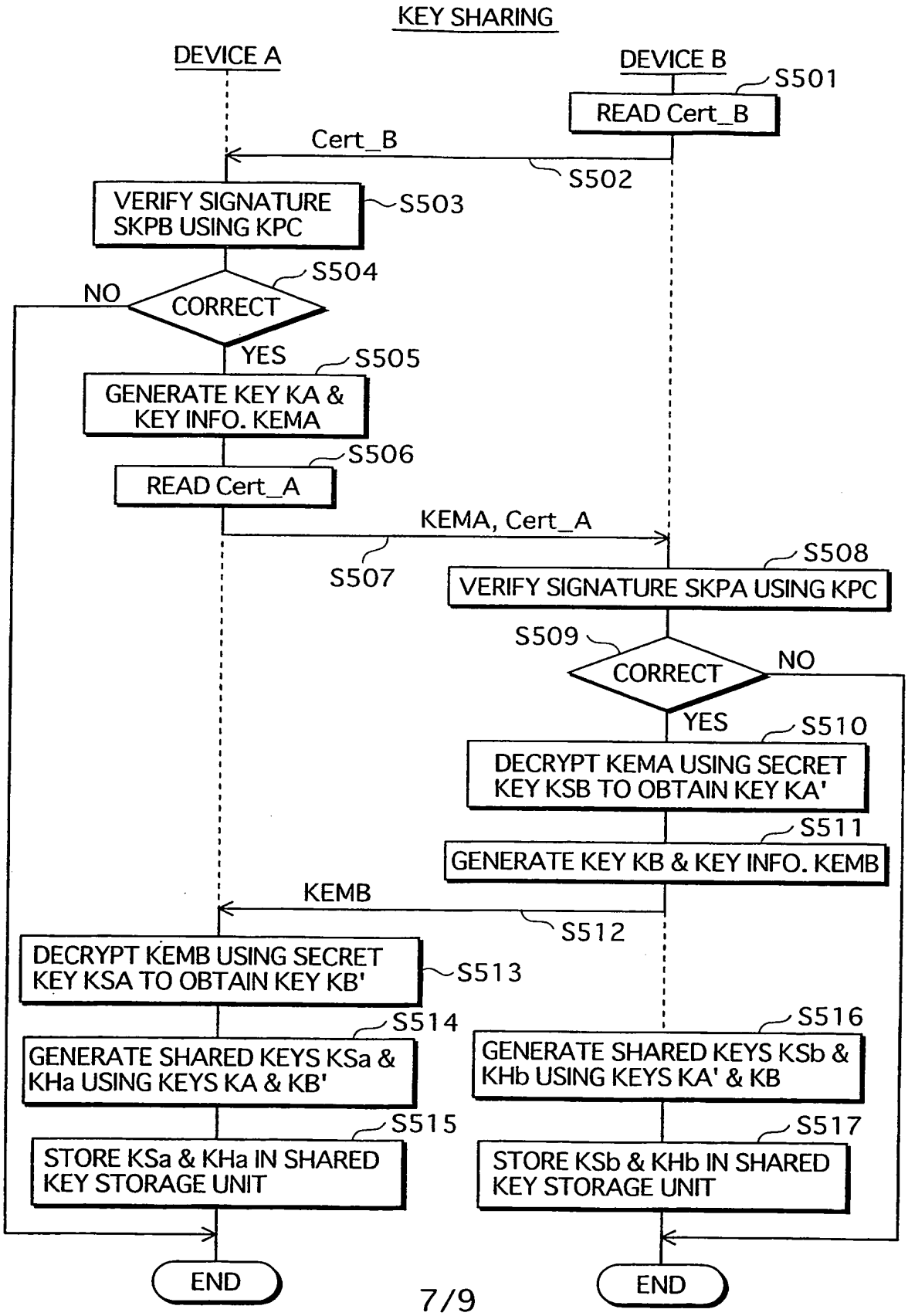

KEY SHARING
DEVICE A
DEVICE B
S501
READ Cert_B
Cert_B
S502
VERIFY SIGNATURE SKPB USING KPC
S503
S504
NO
CORRECT
YES
S505
GENERATE KEY KA & KEY INFO. KEMA
S506
READ Cert_A
KEMA, Cert_A
S507
S508
VERIFY SIGNATURE SKPA USING KPC
S509
CORRECT
NO
YES
S510
DECRYPT KEMA USING SECRET KEY KSB TO OBTAIN KEY KA'
S511
GENERATE KEY KB & KEY INFO. KEMB
KEMB
S512
DECRYPT KEMB USING SECRET KEY KSA TO OBTAIN KEY KB'
S513
S514
GENERATE SHARED KEYS KSa & KHa USING KEYS KA & KB'
S516
GENERATE SHARED KEYS KSb & KHb USING KEYS KA' & KB
S515
STORE KSa & KHa IN SHARED KEY STORAGE UNIT
S517
STORE KSb & KHb IN SHARED KEY STORAGE UNIT
END
END

FIG.8

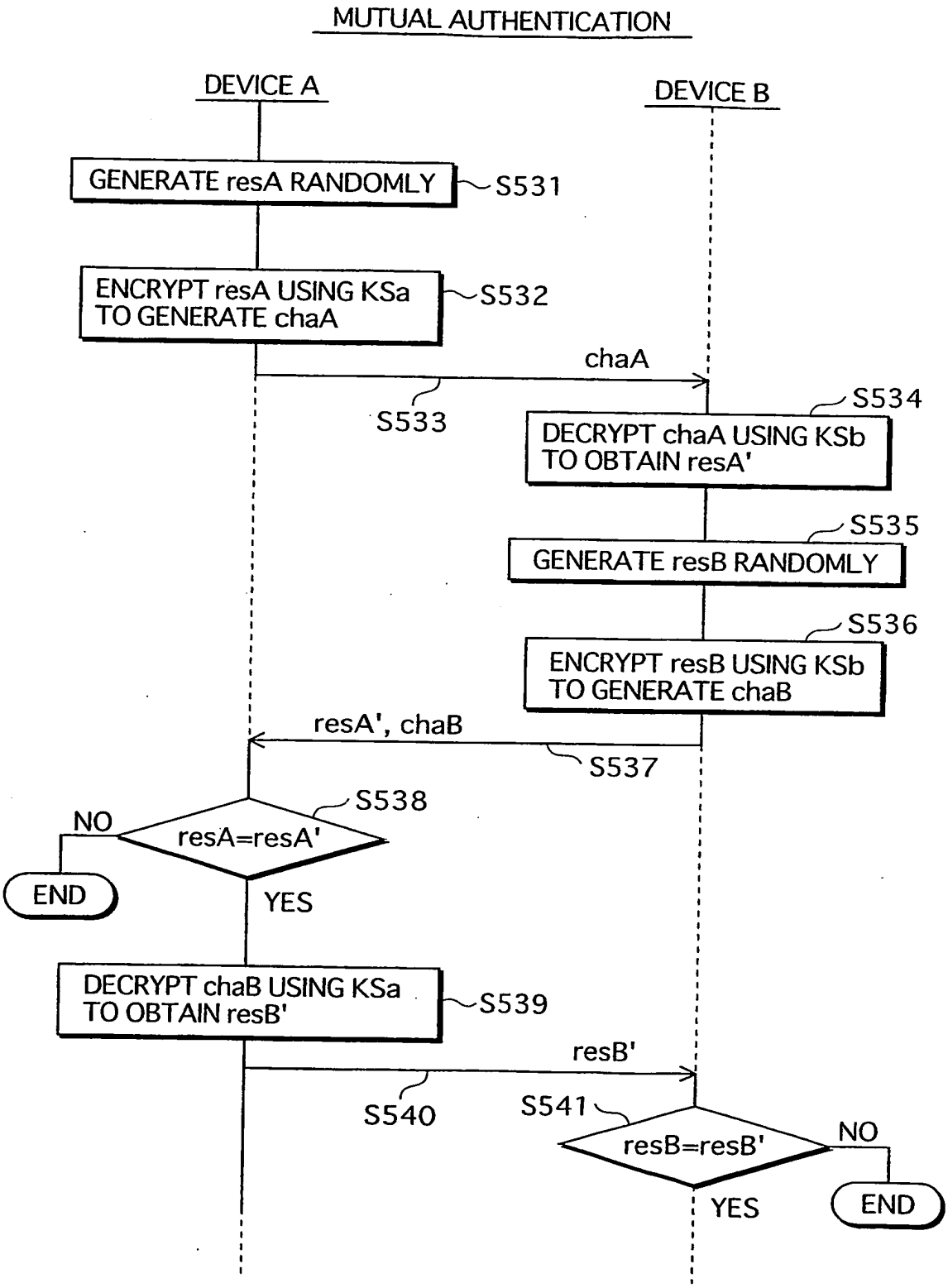
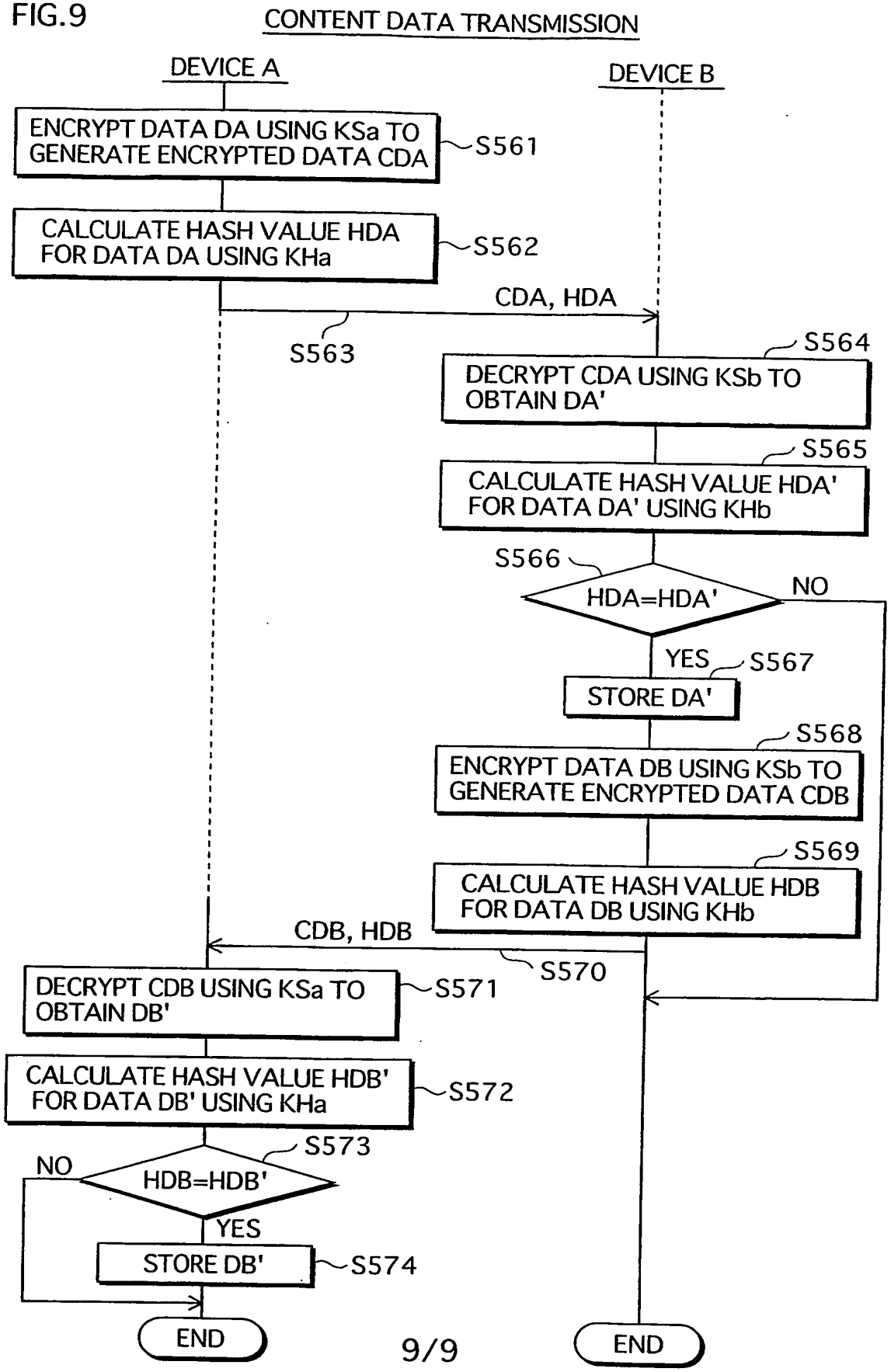

MUTUAL AUTHENTICATION
DEVICE A
DEVICE B
GENERATE resA RANDOMLY
S531
ENCRYPT resA USING KSa TO GENERATE chaA
S532
chaA
S533
S534
DECRYPT chaA USING KSb TO OBTAIN resA'
S535
GENERATE resB RANDOMLY
S536
ENCRYPT resB USING KSb TO GENERATE chaB
resA', chaB
S537
S538
resA=resA'
NO
END
YES
DECRYPT chaB USING KSa TO OBTAIN resB'
S539
resB'
S540
S541
resB=resB'
NO
END
YES

FIG.9


CONTENT DATA TRANSMISSION
DEVICE A
DEVICE B
ENCRYPT DATA DA USING KSa TO GENERATE ENCRYPTED DATA CDA
S561
CALCULATE HASH VALUE HDA FOR DATA DA USING KHa
S562
CDA, HDA
S563
S564
DECRYPT CDA USING KSb TO OBTAIN DA'
S565
CALCULATE HASH VALUE HDA' FOR DATA DA' USING KHb
S566
HDA=HDA'
NO
YES
S567
STORE DA'
S568
ENCRYPT DATA DB USING KSb TO GENERATE ENCRYPTED DATA CDB
S569
CALCULATE HASH VALUE HDB FOR DATA DB USING KHb
CDB, HDB
S570
DECRYPT CDB USING KSa TO OBTAIN DB'
S571
CALCULATE HASH VALUE HDB' FOR DATA DB' USING KHa
S572
S573
NO
HDB=HDB'
YES
STORE DB'
S574
END
END